

ABSTRACT

A method of establishing a trusted path of data and a method of verifying the integrity of data presented for signing to a user of the personalized device in a public-key cryptographic scheme. The method comprises establishing a trusted path between the user and secure module residing on the personalized device. The secure module holds the user's private key, displays information about the data message directly to the user, and generates the signature only when instructed to do so. The decision whether or not to sign the data message is determined by the user.